SOFTWARE ASSURANCE HIGHLIGHTS

February 2012

Software Security Automation News

With DHS NCSD Software Assurance (SwA) Program sponsorship and MITRE technical lead:

CVE Use Increased.

- 340 new Common Vulnerabilities and Exposures (CVE) Identifiers were added to the public CVE List in February for a total of 49,269 usable identifiers now available. CVE enables continuous monitoring, threat reporting, and other cybersecurity programs, and it is included in the 2012 Federal Information Security Management Act (FISMA) reporting metrics for Federal agencies to use in their annual reporting to the Office of Management and Budget (OMB) and the White House.
- Three additional information security products completed the CVE Compatibility Process. A total of 126 products from 69 organizations are now recognized as Officially CVE-Compatible. Three more firms declared their information security products to be CVE compatible. A total of 106 organizations to-date have made declarations of CVE Compatibility for 174 products and services.
- CVE was mentioned in a January 9th article entitled "Getting the Most Out of Automated IT Security Management" on Government Computer News.com.

OVAL Adoption Increased.

- Two more products achieved the second phase of the Open Vulnerability and Assessment Language (OVAL) Adoption process. Now 17 products from 12 organizations are recognized as Official OVAL Adopters. 23 organizations to-date have made declarations to adopt OVAL for 32 products and services. Eight organizations are now hosting repositories of OVAL content in addition to the OVAL Repository at MITRE.

CWE Adoption Increased.

- 13 products from 5 organizations were recognized as being "Officially Common Weakness Enumeration Compatible (CWE-Compatible)." These information security products were the first-ever to achieve the final stage of the CWE Compatibility Process.
- The National Institute of Standards and Technology (NIST) declared that its Web-based software security assurance application, Software Assurance Metrics and Tool Evaluation (SAMATE) Reference Dataset (SRD), is CWE-Compatible.
- 2 more products declared their CWE compatibility. A total of 28 organizations to-date have made Declarations of CWE Compatibility for 46 products and services.

MAEC Updated to Incorporate CybOX

- Further updates to the Malware Attribute Enumeration and Characterization (MAEC) Language incorporated the use of Cyber Observable eXpression (CybOX). MAEC Version 2.1 will soon be released.

ITU-T Adopted SwA Security Automation in CYBEX X.1500 Standards

DHS NCSD Global Cyber Security Management (GCSM) programs for SwA and Research and Standards Integration (RSI) have has been participating in and contributing to the work of the International Telecommunication Union – Telecommunication (ITU-T) Standardization Sector since Fall 2009, primarily in Study Group I7 (SG 17) (Security) Question 4 (Q.4) (Cybersecurity). GCSM's focus in Q.4 has been in the development of standards related to Cybersecurity Information Exchange (CYBEX X.1500 series), which are of particular interest to NCSD. These standards will enable coherent, comprehensive, global, timely, and trusted exchange of cybersecurity information, and provide for the structured discovery and interoperability of that information, as envisioned by the DHS Blueprint for a Secure Cyber Future and the DHS cyber ecosystem white paper titled "Enabling Distributed Security in Cyberspace." The recently approved ITU-T recommendation added a work item on continuous monitoring that advocates the use of GCSM SwA-sponsored security automation enumerations and languages (e.g., CVE, CAPEC, CWE, MAEC, OVAL, and CWSS), and others sponsored by NSA and NIST.

CybOX Received Wider Recognition for Sharing Indicators and Information

The Cyber Observable eXpression (CybOX) was mentioned in a February 1st SC Magazine.com article entitled "Information Sharing Grows Up." The author states, "Efforts, such as MITRE's Cyber Observable Expression (CybOX), are the kinds of toolkits needed to facilitate machine- and human-readable content exchange." Conclusion indicated: "Sharing information within a community of trust is the best defense you can give your organization to thwart … attacks."

Software Assurance Forum at MITRE, McLean VA the week of March 26th

With themes addressing Security Automation, Mobile Security and Trustworthy Cyberspace, the SwA Forum will be held March 26 - 28, 2012 at MITRE in McLean, Virginia. Keynote presentations by DHS NCSD's John Streufert and NSA's Tony Sager will open the Tuesday track, and keynote presentations by DHS S&T's Doug Maughan and Cigital's Gary McGraw open the Wednesday track. Tutorials on CybOX, MAEC, OVAL, and other security automation efforts will be presented on March 26, 2012. NIST will host their Static Analysis Tools Exposition (SATE) on March 29. The event is open to the public and FREE, but registration is required;

SOFTWARE ASSURANCE HIGHLIGHTS

February 2012

(send details to: softwareassurance@asballiance.com). For more information see: https://buildsecurityin.us-cert.gov/bsi/events/1293-BSI.html.

The SwA Forum will include the following tracks:

Tutorials on eXchanging Indicators and Information for Incident Response

Monday, March 26th

The technical mechanisms for sharing and exchanging indicators and information about incidents within communities support the Blueprint for a Secure Cyber Future (to be covered on Wednesday). These capabilities will allow for the integration of open international standards for interoperable security automation and improve communications between incident responders, cyber security managers, and software developers. This track will cover the individual standardization efforts including CybOX, the Common Attack Pattern Enumeration and Classification (CAPEC), and the Malware Attribute Enumeration and Characterization (MAEC), along with the Common Event Expression (CEE) and the Incident Object Description and Exchange Format (IODEF). The components that enable indicator exchange were developed collaboratively with community stakeholders such as MITRE, the US Computer Emergency Readiness Team (US-CERT), and the National Security Agency (NSA). This type of sharing infrastructure enables some of the automation required of Federal agencies by the Federal Information Security Management Act (FISMA).

Securing a Mobile World

Tuesday, March 27th

The challenge of securing the mobile world is complex and therefore requires multi-disciplinary solutions. Existing security models are not sufficient to meet the information protection needs of an enterprise. Application developers, system and network administrators, and incident responders need to collaborate to address mobile computing risk. To be effective, this collaboration requires rapid sharing of standardized threat and vulnerability information so public and private stakeholders can act quickly to mitigate risks to their operations and activities. Additionally, threats from new types of attacks and the proliferation of malware in applications pose significant challenges, especially to "Bring Your Own Device" (BYOD) environments. This track will discuss these challenges and potential solutions, beginning with keynote presentations by representatives of leading mobile platforms followed by a panel on securing mobile operating systems.

Keynote Speakers on Tuesday 27 March

- John Streufert, Director, National Cyber Security Division (NCSD), Office of Cybersecurity and Communications (CS&C), National Protection and Programs Directorate (NPPD), Department of Homeland Security (DHS)
- Tony Sager, Chief Operating Officer, Information Assurance Directorate, National Security Agency

Software Assurance Enabled Trustworthy Cyberspace

Wednesday, March 28th

The global economy has become dependent on cyberspace due to a sharply growing share of world commerce being transacted there. Yet our critical infrastructure–such as the electricity grid, financial sector, and transportation networks that sustain our way of life–has suffered repeated cyber intrusions, and cyber-crime has increased dramatically over the last decade. As a consequence, the President has thus made cybersecurity an Administration priority. When the President released his Cyberspace Policy Review two years ago, he declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation." This track will highlight the latest initiatives to establish a Trustworthy Cyberspace and Software Assurance's (SwA) role and potential in those initiatives.

Keynote Speakers on Wed 28 March

- Gary McGraw, Chief Technology Officer, Cigital, Inc. on "Building Security In Maturity Model (BSIMM)"
- Douglas Maughan, Director, Cyber Security Division, Science and Technology Directorate, Department of Homeland Security (DHS)

How NIST's Special Publication 800-53 Addresses Software Assurance

In the past, vulnerabilities in IT systems were largely mitigated by security, network, and/or other operational support teams. They have succeeded to the point that attackers have shifted their strategies to exploitable software. Consequently, development teams must be part of the process to prevent weaknesses rather than remediate vulnerabilities. The recently released Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program identifies Designed–In security as new theme focused

on building "the capability to design, develop, and evolve high-assurance, software-intensive systems predictably and reliably while effectively managing risk, cost, schedule, quality, and complexity." The February 2012 draft of NIST SP 800-53 rev 4 includes additional controls that provide explicit guidance for addressing application security in the development lifecycle. This panel will provide an update on NIST SP 800-53 rev 4 and provide the attendees with specific resources currently available through the SwA Community to effectively implement the controls.

Static Analysis Tools Exposition (SATE)

Thursday, March 29th
Finding Truth in the Juliet Source Code Analysis Tool Test Suite and CVEs

Software must be developed well to have high quality: quality cannot be "tested in." However auditors, certifiers, and others must assess the quality of software they receive. Static analyzers are capable and are developing quickly, yet, we need far more. This workshop gathers participants and organizers of SATE IV to share experiences, report interesting observations, and discuss lessons learned. This is the first chance the public will have to hear our observations and preliminary conclusions. The target programs chosen include four large, open-source tools selected for having known (CVE-reported) vulnerabilities and also most of the Juliet test suite, almost 60,000 synthetic test cases in C/C++ and Java. Another goal of the workshop is to convene researchers, tool developers, and government and industrial users of software assurance tools to define obstacles to urgently-needed SwA capabilities and identify engineering or research approaches to overcome them. There is also an opportunity for attendees to help shape the next exposition, SATE V. NIST's Paul Black will lead this track.

SwA Forum Call for Participation for Fall 2012 sessions

Proposals are welcomed for the Fall 2012 Software Assurance Forum during the week of September 17, 2012 at MITRE-1, McLean, Virginia. DHS CS&C NCSD is again co-sponsoring this event with the Department of Defense (DoD) Office of the Secretary of Defense (OSD) and National Institute for Standards and Technology (NIST) Information Technology Laboratory.

The SwA Forum brings together members of government, industry, and academia with vested interests in software assurance to discuss and promote integrity, security, and reliability in software. Progress updates on relevant programs and initiatives will be presented. If you are implementing practical solutions to problems related to examining alternatives to mitigate security risks attributable to software, then you should consider participating in a panel or giving a presentation at the Software Assurance Forum to enable others to secure their part of cyber space. We are soliciting submissions in a number of different categories for this SwA Forum. We are especially interested in submissions that address the applied technology and lessons learned in the area of Software Assurance. DHS is not providing financial support for SwA participants. If you are interested in participating, please send an email to software.assurance@dhs.gov.

Call for Articles for September/October 2012 issue of CrossTalk

The Sep/Oct 2012 issue of *CrossTalk* Journal of Defense Software Engineering will have the theme "Resilient Cyber Ecosystem" – the DHS NCSD SwA program is co-sponsoring this issue and invites you to provide an article. Articles are due April 10, 2012. See http://www.crosstalkonline.org/submission-guidelines/ for submission guidelines.

SOFTWARE ASSURANCE HIGHLIGHTS

February 2012

IEEE SWEBOK V3 review

The IEEE Computer Society is now soliciting public review comments on three knowledge areas (KAs) for Version 3 of the Guide to the Software Engineering Body of Knowledge (SWEBOK V3). SWEBOK V3 is an update to the 2004 version of the SWEBOK Guide, which is also known as Technical Report ISO/IEC TR 19759. The 15 KAs in SWEBOK V3 are being published incrementally as they become available for review. Three new KAs are now available for review (Software Engineering Methods and Models, Software Maintenance, and Mathematical Foundations). These KAs can be reviewed and comments can be submitted at: http://computer.centraldesktop.com/swebokv3review/. The SwA Community can still influence the SWEBOK to better ensure SwA will be properly reflected. Please send an email to software.assurance@dhs.gov with your comments so that we can follow up.

Learning from Authoritative Security Experiment Results Workshop

March 26th is the submission deadline for LASER 2012—the Learning from Authoritative Security Experiment Results workshop. You can find out more about the workshop at http://www.laser-workshop.org. The purpose of this workshop is to quickly identify and learn from both success and failure, so unexpected results are welcome. Unfortunately, papers reporting on experiments with unanticipated results that the experimenters cannot explain, or experiments that are not statistically significant, or engineering efforts that fail to produce the expected results, are frequently not considered publishable, because they do not appear to extend our knowledge. Yet, some of these "failures" may actually provide clues to even more significant results than the original experimenter had intended. The research is useful, even though the results are unexpected. Please send us your nominations via email to Software.Assurance@dhs.gov.

ICSQ Call for Participation

The International Conference on Software Quality 2012 is seeking speakers. The conference this year is October 30-31, 2012 in Indianapolis, Indiana with pre-conference tutorials on October 29, 2012. The website is www.icsq.com. The SwA Community has been asked to propose 10 sessions for two days of SwA tracks, with the possibility of tutorial(s) on day one. Please send an email to software.assurance@dhs.gov if you are interested in participating. DHS is not providing financial support for SwA speakers.

Call for Comments on SwA Pocket Guides

The SwA Pocket Guides at https://buildsecurityin.us-cert.gov/swa/pocket_guide_series.html are free, downloadable documents on SwA in acquisition and outsourcing, SwA in development, the SwA life cycle, and SwA measurement and information needs. SwA Pocket Guides are developed collaboratively by participants in the SwA Forum and Working Groups, which function as a stakeholder community that welcomes additional participation in advancing and refining software security. The SwA team has requested a call for comments and suggestions on the following pocket guides: "*Architecture and Design Considerations for Secure Software*," "*Secure Coding*," and "*Requirements Analysis for Secure Software.*" The current drafts of the pocket guides have significant updates compared to the ones on the Community Resource and Information Clearinghouse. Contact Software.Assurance@dhs.gov to receive current drafts of these recently revised pocket guides.

SwA Websites Offer More Content

The DHS-sponsored websites "Build Security In" https://buildsecurityin.us-cert.gov/bsi and Software Assurance Community Resources & Information Clearinghouse https://buildsecurityin.us-cert.gov/swa were updated with collaboratively developed material.

The DHS NCSD Software Assurance (SwA) Program leads efforts in software security automation, diagnostics, measurement, and indicator information sharing efforts through its sponsored projects for Common Attack Pattern Enumeration and Classification (CAPEC), Malware Attribute Enumeration and Characterization (MAEC), Cyber Observables (CybOX), Common Vulnerabilities and Exposures (CVE), Open Vulnerability and Assessment Language (OVAL), and Common Weakness Enumeration (CWE) that includes the Common Weakness Risk Analysis Framework (CWRAF) and Common Weakness Scoring System (CWSS).
See details for security automation standardization efforts at "Making Security Measurable" http://measurablesecurity.mitre.org,

The DHS NCSD SwA Program provides the infrastructure for public-private community collaboration and advances relevant standards, education and training, and it provides resources to reduce software vulnerabilities; share information, and improve capabilities to routinely develop, acquire and deploy resilient software products and services. See "Build Security In" https://buildsecurityin.us-cert.gov/bsi, and SwA Community Resources & Information Clearinghouse https://buildsecurityin.us-cert.gov/swa,